UNIVERSITY OF SOUTHAMPTON

Applying Gamification to Teaching Cyber Security

By

Reece Buckle

Project Supervisor: Dr Nawfal Fadhel

Second Examiner: TBA

A project progress report submitted for the award of BSc Computer Science

Department of Electronics and Computer Science

Novemeber 2020

Abstract

To write last

Statement of Originality

- I have read and understood the ECS Academic Integrity information and the University's Academic Integrity Guidance for Students.
- I am aware that failure to act in accordance with the Regulations Governing Academic Integrity may lead to the imposition of penalties which, for the most serious cases, may include termination of programme.
- I consent to the University copying and distributing any or all of my work in any form and using third parties (who may be based outside the EU/EEA) to verify whether my work contains plagiarised material, and for quality assurance purposes.

You must change the statements in the boxes if you do not agree with them.

We expect you to acknowledge all sources of information (e.g. ideas, algorithms, data) using citations. You must also put quotation marks around any sections of text that you have copied without paraphrasing. If any figures or tables have been taken or modified from another source, you must explain this in the caption and cite the original source.

I have acknowledged all sources, and identified any content taken from elsewhere.

If you have used any code (e.g. open-source code), reference designs, or similar resources that have been produced by anyone else, you must list them in the box below. In the report, you must explain what was used and how it relates to the work you have done.

I have not used any resources produced by anyone else.

You can consult with module teaching staff/demonstrators, but you should not show anyone else your work (this includes uploading your work to publicly-accessible repositories e.g. Github, unless expressly permitted by the module leader), or help them to do theirs. For individual assignments, we expect you to work on your own. For group assignments, we expect that you work only with your allocated group. You must get permission in writing from the module teaching staff before you seek outside assistance, e.g. a proofreading service, and declare it here.

I did all the work myself, or with my allocated group, and have not helped anyone else.

We expect that you have not fabricated, modified or distorted any data, evidence, references, experimental results, or other material used or presented in the report. You must clearly describe your experiments and how the results were obtained, and include all data, source code and/or designs (either in the report, or submitted as a separate file) so that your results could be reproduced.

The material in the report is genuine, and I have included all my data/code/designs.

We expect that you have not previously submitted any part of this work for another assessment. You must get permission in writing from the module teaching staff before re-using any of your previously submitted work for this assessment.

I have not submitted any part of this work for another assessment.

If your work involved research/studies (including surveys) on human participants, their cells or data, or on animals, you must have been granted ethical approval before the work was carried out, and any experiments must have followed these requirements. You must give details of this in the report, and list the ethical approval reference number(s) in the box below.

My work did not involve human participants, their cells or data, or animals.

ECS Statement of Originality Template, updated August 2018, Alex Weddell aiofficer@ecs.soton.ac.uk

Contents

1 Introduction **4**
- 1.1 Problem Summary . . . 4
- 1.2 Goals & Scope . . . 4

2 Literature Review & Research **6**
- 2.1 Introduction . . . 6
- 2.2 The Problem with Current Cyber Security Training Programs . . . 6
- 2.3 A Critical Analysis of Pre-Existing Cyber Security Games . . . 6
  - 2.3.1 Web Applications . . . 7
  - 2.3.2 Video / Simulation . . . 7
  - 2.3.3 Cooperative Tabletop . . . 7
  - 2.3.4 Task Management . . . 8
  - 2.3.5 Single Player . . . 8
- 2.4 Difficulties that Pre-Existing Cyber Security Games Face . . . 8
- 2.5 Why Use a Game-Based Learning Approach? . . . 9
- 2.6 Conclusion . . . 9

3 The Proposed Final Design **10**
- 3.1 Proposed Idea . . . 10
- 3.2 A Justification of this Approach . . . 10
- 3.3 Functional Requirements . . . 10
- 3.4 Non - Functional Requirements . . . 11
- 3.5 A Brief Account of Work to Date . . . 11

4 A Plan of Remaining Work & Project Planning **12**
- 4.1 Remaining Work . . . 12
- 4.2 Project Management Tools & Techniques . . . 12
- 4.3 Gantt Chart for Phase 1 . . . 13
- 4.4 Gantt Chart for Phase 2 . . . 14
- 4.5 Risk Assessment . . . 15

5 Bibliography **16**

6 Appendices **17**
- 6.1 A Review of Cyber Security / Serious Games . . . 17

1 Introduction

1.1 Problem Summary

Problem Statement

Despite the existence of many cyber security awareness programs, there is still a lack of effective, widespread cyber security training

As modern day technology is ever evolving, the number of users who interact with technology on a daily basis increases consequently. As a result, the risk of an individual, or business, begin targeted by cyber-crime increases proportionately. In particular, small and medium-sized businesses (SMBs) are the biggest sectors which are hit hardest by cyber-crime [1], which stem from a variety of causes including budget restraints and a general ignorance towards the importance of cyber security.

In fact, as a consequence of COVID-19 changing the dynamic of industry standards this year, a statistical analysis of all cyber-crimes targeting individuals May 2020 has increased by an average of 43% in comparison with the previous year [2]. Furthermore, this new trend in targeted hacking of individuals, which has increased by 77.41% [2]), has arisen from the fact that employees are encouraged to work from home via their personal computers. Consequently this has fed into a new strategy whereby cyber-criminals are moving laterally into organisational infrastructure by targeting and infecting employees at their less secure personal computers [3].

In regards to this problem, this paper will explore the effectiveness of educational games - which has been shown to have an advantage on the learning outcome in comparison with traditional training material [4]. Therefore this paper presents the following research question and hypothesis:

Research Question

Does teaching cyber security through a gamified medium improve user confidence in protecting against cyber attacks?

Hypothesis

Creating an educational cyber security game will leave users feeling more confident and effective in protecting themselves against cyber attacks.

1.2 Goals & Scope

The goal of this project is to investigate how to effectively apply gamification mechanics in order to teach cyber security principles appropriately. The expected result of this project is to create a multiplayer, online tabletop board game in which the impact of said game can be measured and analysed. To date, this report

includes an evaluation of literature review pertaining to pre-existing educational cyber security games as well as current trends in cyber security training and mechanics for game-based learning. This project will incorporate a variety of core game mechanics, [5], including:

- Avatar / User Profile
- Badges / Privileges
- Challenge
- Competition
- Collaboration
- Feedback / Guidance
- Goals / Objectives
- Incentives / Rewards
- Leaderboards
- Points System
- Progress / Levels
- Role Playing
- Story
- Tips / Hints System

2 Literature Review & Research

2.1 Introduction

In order to gain valuable insight, a variety of papers were read in regards to pre-existing cyber security training / awareness programs, pre-existing serious cyber security games, table top games for education (card and board games) and finally gamification techniques and mechanics.

2.2 The Problem with Current Cyber Security Training Programs

This report will specifically analyse the shortcomings and difficulties that relate to current training programs designed for businesses and (SMEs) [1, 6].

Problem	Description
1	SMEs can be heavily constrained by a limited budget
2	SMEs can be difficult to reach as they do not understand the severity of data breaches
3	Users are able to play a full version of the game
4	SMEs are often distracted by the operational requirements for setting up and running a small business
5	SMEs struggle to identify their assets in terms of the risk associated with it
6	TODO
7	TODO
8	TODO

In regards to the delivery of training programs, providing generalised cyber security advice (from an independent advisor) has been shown to have little effect on changing the behaviour / awareness of employees within SMEs [1, 7]. Furthermore, traditional training methods/simulations are generally undertaken in a formal environment which leads to a situation of recipients not absorbing the information well [2].

The method / scenario of cyber security exposure is also important as whilst employees may understand some general information about the vulnerability / attack demonstrated, they may still fail to see how it relates to their workplace environment [6] or how they link together in a multifaceted social engineering attack [7].

2.3 A Critical Analysis of Pre-Existing Cyber Security Games

For a full account of educational games and resources reviewed, please see Appendix A. My methodology for reviewing cyber security games was two fold:

- First - utilising the Google search engine with the following keywords: 'cyber security', 'serious games', 'gamification' and 'game-based learning' in order to look for any widely available games. These commonly returned web applications designed for students in both lower and higher education.
- Second - utilising Google Scholar and the IEEE Database with the same keywords in order to find academic papers which either reviewed other educational games, or were demonstrating one. For the games that were not available to play online, I summarised the key information based from the academic source material.

Following this, I concluded the different categories of educational game based learning in order to identify the most appropriate for the purpose of answering the research questions established in this project.

2.3.1 Web Applications

Advantages	Disadvantages
Simple point and click interactivity	Can lack depth and relevance to a specific target demographic
Very accessible with an internet connection	Not suitable for offline usage
Relatively cheap development cost / time	

2.3.2 Video / Simulation

Advantages	Disadvantages
Contextually appropriate for use within the workplace [6]	Not appropriate for other demographics
Accessible online/offline	Requires multiple play-throughs if scenarios are divergent
	Typically not very fun as undertaken in a formal environment [6]

2.3.3 Cooperative Tabletop

Advantages	Disadvantages
Encourages social engagement and team-working	Requires multiple players
Cheap to prototype a physical implementation	Requires much fine-tuning of rules and mechanics implemented
Encourages thinking strategically	

2.3.4 Task Management

Advantages	Disadvantages
Easy to employ around current learning strategies (within the classroom or workplace)	Requires long term evaluation of effectiveness
Good example of procedural learning [8]	Not a true application of an educational game

2.3.5 Single Player

Advantages	Disadvantages
Immersive and engaging typically through story driven content	High development cost / time
Often places the player as a white hat / black hat hacker which encourages adversarial thinking	Doesn't explore how to patch / prevent vulnerabilities as a target

2.4 Difficulties that Pre-Existing Cyber Security Games Face

Many of the educational games reviewed relied heavily on presenting facts and then subsequently quizzing the user with a related question. However, users with common sense can rule out incorrect answers which fail to invoke critical thinking and keep the user engaged. As a solution, gamified strategies should incorporate a variety of factual, conceptual and procedural learning methodologies [8] especially due to the rapidly changing landscape of cyber security in which cyber-criminals will always be engineering new attack vectors so it is imperative for end-users to understand the concepts and adapt their way of thinking when interacting with new technology.

For conceptual learning, rather than simply quiz the player on their ability to perform fact recall, the game should instead explore basic concepts in a stimulating way - i.e why it is extremely important to use strong passwords and 2 factor authentication.

For procedural learning, both Nova Cyber Lab and Classcraft (Appendix A) exemplify this by starting off with simple challenges and progressively increasing the difficulty of said challenges as the user progresses. Unlike the other games reviewed, Classcraft is unique as it encourages users within a team to continually expand upon their knowledge by working towards new goals and objectives collaboratively. Furthermore, this system incorporates real-world rewards and punishments to encourage user-engagement.

Finally, many serious cyber security games are designed primarily for university students and businesses but are not readily available to the general public [8]. In fact, my own research correlates with this - whereby many of the publicly acces-

sible educational games reviewed were considerably outdated and rarely relevant for the general public.

2.5 Why Use a Game-Based Learning Approach?

Because it's fun! The main pitfalls from educating businesses often occur as the delivered training material can feel as another tedious task in which the employee is expected to complete within working hours and desires to complete as fast as possible [7]. This absentmindedness results in training content which is not absorbed effectively [1, 7]. Furthermore, [4] provides evidence that game-based learning can be much more effective in comparison to equivalent traditional training methods and schemes.

Some key strengths to game based learning [4] include:

- Rapid progress paired with instant feedback
- Excels in user engagement
- Allows the user to learn from mistakes in a safe, non punishing environment
- Serve as a platform to encourage self-learning at the user's desired pace
- Allows the user to become deeply immersed into the 'game - world' where learning feels like a secondary objective
- Relatively cheap and low cost to produce in comparison to larger training schemes
- Easy to distribute among multiple platforms (if software) or incorporate into the workplace (for physical implementations)

2.6 Conclusion

To summarise, cyber security training programs need to be cost effective and target the specific needs and requirements of the workplace to be effective for SMEs. Furthermore, these requirements are often identified via a risk assessment in which an appropriately designed board game could make employees who interact with said game aware of newly found threats.

3 The Proposed Final Design

3.1 Proposed Idea

The proposed application is a 2-4 multiplier board game. As previously identified, cooperation/competition are two of the strongest mechanics when incorporated in serious games, since typically cyber security training simulations / games are often till not very engaging or fun when played alone (also as an observation from my research).

The application will loosely be inspired from Mario Party's format, in which players will roll a dice to move around a map. An intial map idea is to be situated within a working office where the goal is to reach significant objects (such as locate a server room / dumpster dive files binned in the reception / locate an infected memory stick etc). In the process of moving, players may land on optional item tiles which will drop a defence or attack card respectively. These cards can be used to handicap other players if they are not holding the relevant defence card. Between each round (or if a player lands on a certain tile), a mini-game challenge pertaining to cyber security will be triggered in which the players can compete against each-other.

See Appendix [x] for outline game design template for the proposed project.

3.2 A Justification of this Approach

Some lit review lines here about cyber security board games

From review of a toolkit for creating these types of serious games, the following gamification mechanics have been identified as appropriate for this application:

3.3 Functional Requirements

Requirement	Description
Multiplayer	Users are able to play in turns with other users
Web Accessible	Users are able to access the the game lobby from their web browser
Game is Playable	Users are able to play a full version of the game
Account Registration	Users are able to register and login (with safe password hashing and authentication)
Save Profile	Users profiles are saved (and earned achievements integrated with MySQL)
Achievements	Users are able to earn achievements from progress
Score / Leaderboard	Users can see their score vs other players
Single Player Mode	Users can play single player (versus computer AI)

3.4 Non - Functional Requirements

Requirement	Description
Availability	The application should be accessible on both desktop web browsers and via mobile tablets
Ease of use	The application should be easy to learn and understand
Accessibility	The application should cater for disabilities such as colour blindness
Security	The application should be secure and protect user's credentials should account registration be implemented
Factually Correct	The application should be factually correct in any cyber security concepts explored
Performance	As a web browser game, it should be relatively smooth to both play and load (with quick multiplayer response times). However, latency is less of an issue given the turn-based mechanic.
Scalability	Should be able to deal with 2-4 connected users per game

3.5 A Brief Account of Work to Date

- Appropriate mechanics have been identified and researched from pre-existing serious cyber security games and literature review
- Appropriate Game Engine (Unity), cloud services (Photon Engine) and APIs have been identified in order to create and host the game
- Cyber security vulnerabilities, game - objects and mini-game ideas for the final implementation have been brainstormed
- A wire-frame of the game interface and UI has been mocked up // REMOVE THIS IF NOT COMPLETE IN TIME

4 A Plan of Remaining Work & Project Planning

4.1 Remaining Work

Task / Requirement	MoSCoW	Difficulty
Establish Multiplayer Networking	Must	High
Web Browser Accessible	Should	Medium
Logic for Turn Based Movement	Must	Medium
Add Graphics / Sound Assets	Must	Low
Add Cyber Attack / Defence Items	Must	Low
Add Objectives / Goals	Must	Low
Add Minigame Tiles / Rounds	Should	High
Add a Score / Leaderboard	Should	Low
Account Registration	Could	Medium
Save Profile	Could	Medium
Add Achievements	Could	Low
Test the Application	Could	High
Complete the Application Sufficient for Review	Must	Very High
Obtain Feedback / Research Effectivity of Product	Should	Medium
Single Player Mode (with AI)	Won't	Very High

Single player mode is a desirable feature however as identified in the literature review, multiplayer is more appropriate in the context of a board game.

4.2 Project Management Tools & Techniques

Tools	Description
Southampton GitLab	Ability to share a visual representation of tasks completed via GitLab's Boards, Issues and Milestones as well as handle version control
Trello	Visual representation for setting daily/weekly tasks
Workona	Chrome extension for streamlining online research into a succinct workplace
Menderley	Reference management for supporting literature
Google Drive	Cloud storage for research, recording minutes and sharing documents
Unity Engine	Game engine for developing an application for the Web (WebGL)
Photon	Cloud service for hosting multiplayer servers online
Vagrant	Establishing a virtual software development environment

4.3 Gantt Chart for Phase 1

Week Beginning	1	2	3	4	5	6	7	8	9	10
Date beginning	**Oct 5**	**Oct 12**	**Oct 19**	**Oct 26**	**Nov 2**	**Nov 9**	**Nov 16**	**Nov 23**	**Nov 30**	**Dec 7**
Planning										
Project Brief										
Literature Review										
Submit Project Brief		x								
Project Planning / Gantt Draft										
Form Hypothesis / Research Question										
Research										
Review Gamemaking Toolkit										
Research Pre-Existing Cyber Security Games										
Research Game Mechanics										
Brain Storm Game										
Research Dev Tools/Languages/APIs										
Write Progress Report										
Submit Report										x

4.4 Gantt Chart for Phase 2

The proposed schedule for semester 2 accounts for a two-week examination period and aims to finish 5 weeks before the deadline; this allows for a buffer if any part of the project takes more time than anticipated. The final report and application testing will be progressed alongside the implementation period.

Week Beginning	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
Date beginning	**14/12**	**21/12**	**28/12**	**4/1**	**11/1**	**18/1**	**25/1**	**1/2**	**8/2**	**15/2**	**22/2**	**1/3**	**8/3**	**15/3**	**22/3**	**29/3**	**5/4**	**12/4**	**19/4**	**26/4**
Implementation				**Exams**																
Wireframes of Board/UI																				
Set Up Dev Envrionment																				
Set Up Multiplayer Networking (Photon)																				
Create Board Outline																				
Turn Based Logic																				
Graphics / Sound Assets																				
Attack / Defence Items																				
Add Objectives / Goal																				
Minigame Tiles / Rounds																				
Score Board																				
Login Authentication																				
Profile / Achievements																				
Testing / Evaluation																				
Write Unity Test Cases																				
Obtain Ethics Approval																				
Obtain Feedback from Playtesters																				
Analyse Feedback																				
Write Final Report																				
Submit Final Report																				**x**

4.5 Risk Assessment

Risk	Prob (1 - 5)	Severity (1 - 10)	Risk Exposure (P X S)	Mitigation
Project deadlines not met	3	10	30	Weekly meetings with project supervisor to continuously evaluate progress and apsiring to finish 5 weeks early in order to provide a buffer period
Not obtaining Ethics Approval in time	3	9	27	Submit identified research questions before the beginning of Semester 2
Online Multiplayer not being possible due to limitations/pricing of cloud server hosting	3	8	24	Possibility to incorporate LAN multiplayer functionality by utilising the Unity Mirror API. Failing this, it would suffice to implement multiplayer co-op from the same system
Relevant cyber security principles are not effectively taught	3	7	21	By identifying an appropriate target demographic and the most appropriate cyber security content to teach - through literature review
Over/under estimating scope of implementation	3	7	21	Aspired project is relatively modular whereby smaller features (identified as Could in the MoSCoW analysis can be foregone if required. There is also the alternative of implementing Single Player AI instead of multiplayer functinality
Final project doesn't relate to original problem statement/hypothesis	2	9	18	Continuously referring back to the initial problem statement and hypothesis
Sickness / Flu / Mental Health difficulties from Covid19	2	8	16	By exercising daily and reaching out for support earlier (rather than later)
Complications due to Covid19	5	3	15	Aspired project will have online multiplayer (for remote gameplay), alongside Microsoft Teams / Discord for communication
Gamified mechanics are not appropriately utilised	2	7	14	By identifying key mechanics through literature and game review and prioritise the most fundamentally important for this project
Stolen work/data from: cloud storage account being compromised / downloading ransomware	1	10	10	By using randomally generated passwords and 2FA as well as manually backing up important files weekly (on a harddrive protected by an airgap)
Loss of work/data from: PC breaking / Cloud storage servers failing	1	10	10	Storing a copy of work across multiple platforms (Southampton Git, Locally and Google Drive)

5 Bibliography

[1] M. Bada and J. R. Nurse, "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes)," *Information & Computer Security*, 2019.

[2] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, "Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk," *European Societies*, pp. 1–13, 2020.

[3] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *arXiv preprint arXiv:2006.11929*, 2020.

[4] J.-N. Tioh, M. Mina, and D. W. Jacobson, "Cyber security training a survey of serious games in cyber security," in *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2017, pp. 1–5.

[5] A. T. Forde, "A gamification toolkit for improving cyber security standards adoption," *Computers & Security*, 2020.

[6] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014.

[7] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, p. 73, 2019.

[8] R. Roepke and U. Schroeder, "The problem with teaching defence against the dark arts: A review of game-based learning applications and serious games for cyber security education." in *CSEDU (2)*, 2019, pp. 58–66.

6 Appendices

6.1 A Review of Cyber Security / Serious Games

Game	Cyberland - Cyber Security Challenge
Game Type	Web Application Point and Click
Target Audience	Children, Teenagers, Students (High school - University level)
Description	Cyber Security Challenge UK is an organisation which hosts a variety of mini games (Cyberland), competitions and networking between schools, universities, businesses and government institutes
Key Teachings / Findings	Examples of minigames which teach: - Identifying phishing emails - Command line simulator - Firewall simulator (analyse incoming network activity and grant/deny requests - Database simulator -(remove old accounts, sanitise personal information, check admin clearance) - Coffee shop network simulator (using unprotected networks vs VPN and shoulder surfing) - IoT home simulator - making sure all IoT devices have latest software update - Courthouse simulator - demonstrating cyber security laws and ethics - Cipher cracking simulator - Password strength making game - Data leak mystery solver - Malware simulator (demonstrates different types of malware/ransomware and they work)
Mechanics Identified	• Competition • Feedback / Guidance • Tips / Hints • Story • Goals / Objectives

Game	Game of Threats
Game Type	Multiplatform - (Mobile, Tablet, PC), Multiplayer
Target Audience	Businesses - Employees
Description	Employees are split into teams of attackers and defenders who work together to simulate scenarios of cyber attacks and appropriate responses
Key Teachings / Findings	- Teaches people about cyber security trends and to understand the consequences of cyber attacks and what you can do to mitigate the impacts - Helps people understand the mindset of both attackers and defenders- - Prompts discussion with colleagues in teams to popularise cyber security readiness
Mechanics Identified	● Feedback / Guidance ● Incentives / Rewards ● Competition

Game	Webonauts Internet Academy
Game Type	Web Application Point and Click Side Scroller
Target Audience	Children (aged 7-12)
Description	Puts the player as an astronaut in which they can rank up their status by demonstrating smart and good behaviour
Key Teachings / Findings	Teaches children: - How to be respectful online - How to protect themselves online - Looking for trustful website certificates - Establishing privacy settings on profile - Not giving out and using weak passwords
Mechanics Identified	● Avatar ● Feedback / Guidance ● Tips / Hints ● Badges / Privileges

Game	Targeted Attack
Game Type	Web Application Point and Click
Target Audience	Businesses - Employees
Description	Targeted Attack places you as a CEO in a simulation of business growth and defence from cyber attacks
Key Teachings / Findings	Teaches employees: - Smart and safe decision making - Threat level of different types of cyber attacks and how to mitigate them
Mechanics Identified	● Feedback / Guidance ● Story ● Challenge

Game	Classcraft
Game Type	Web Application, Point and Click, Multiplayer, Productivity - Management
Target Audience	School Students
Description	Classcraft incorporates gamifiication principles through the use of management software to set goals and challenges within a classroom and encourages teamwork between students
Key Teachings / Findings	Teaches employees: - Smart and safe decision making - Threat level of different types of cyber attacks and how to mitigate them
Mechanics Identified	● Avatar ● Leaderboard ● Competition ● Badges / Privileges, ● Feedback / Guidance ● Goals / Objectives ● Incentive / Rewards ● Point Systems

Game	Cyber- security Lab
Game Type	Web Application Point and Click
Target Audience	Businesses - Employees
Description	Allows the player to choose a business they'd like to start and require them to spend defence points in different areas of cyber defence
Key Teachings / Findings	Teaches children via minigames: - how to spot phishing emails - how to construct strong passwords - Simple programming principles
Mechanics Identified	● Avatar ● Achievements ● Progress / Levels ● Point System ● Tips / Hints ● Feedback / Guidance

Game	Keep Tradition Secure
Game Type	Web Application Point and Click
Target Audience	University Students
Description	You are a campus student trying to take down a fictional cyber criminal by making smart cyber security decisions
Key Teachings / Findings	Teaches students: - Smart decision making on campus (using public networks vs campus VPN) - Quiz based - Gives out prizes for student participants
Mechanics Identified	● Tips / Hints ● Feedback / Guidance ● Rewards / Incentives

Game	Hacknet
Game Type	Downloadable, Single Player, Point and Click
Target Audience	Gamers
Description	Hacknet is a paid game (on Steam) which is a terminal-based hacking simulator
Key Teachings / Findings	Teaches player: - How to navigate networks - Search for hidden files/folders - Authorisation bypass - Heavy use of terminal/linux commands in a tutorial environment
Mechanics Identified	● Story ● Progress / Levels ● Feedback / Guidance ● Steam Achievements

Game	Cyber Awareness Challenge
Game Type	Downloadable Training Simulator
Target Audience	Businesses Employees
Description	Single Player simulation of everyday life within the workplace and how to behave safely and responsibly
Key Teachings / Findings	- Teaches employees how to be safe in the workplace - Gives points for correct answers and guidance for both right and wrong answers
Mechanics Identified	● Tips / Hints ● Feedback / Guidance ● Story ● Points System